Testimony of

Center for Digital Democracy
Consumer Federation of America
U.S. Public Interest Research Group (U.S. PIRG)

By Edmund Mierzwinski
U.S. PIRG Consumer Program Director

Before the Subcommittee on Commerce, Trade, and Consumer Protection
Committee on Energy and Commerce
U.S. House of Representatives

Honorable Bobby Rush, Chairman

Legislative hearing examining H.R. ____, the "BEST PRACTICES Act," and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual.

---

22 July 2010

Chairman Rush, Representative Radanovich and members of the committee: My name is Edmund Mierzwinski, Consumer Program Director for the non-profit, non-partisan U.S. Public Interest Research Group. My testimony today is also on behalf of the following consumer and privacy organizations, the Center for Digital Democracy and the Consumer Federation of America.[1]

Thank you for the opportunity to testify before you on the important matter of how information about consumers is collected and used by businesses in the online and offline worlds. This legislative hearing examining H.R. ____, the "BEST PRACTICES Act," and H.R. ____, a discussion draft to require notice to and consent of an individual prior to the collection and disclosure of certain personal information relating to that individual, is very timely. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New technologies allow a web of interconnected businesses – many of which the consumer has never heard of – to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm.

In this testimony, we hope to provide background on why granting consumers greater control of their personal information is critical public policy, why holding data collectors to compliance with the Fair Information Practices matters, and how the new ecology of data collection works. We will then comment on Chairman Rush's proposal, the Best Practices Act, and on another draft bill before the full committee as circulated by members Boucher and Stearns, and how those bills approach the problem and recommendations for improvements.

Our organizations share longstanding concerns for consumer privacy and look forward to working with the committee on these matters. The committee has a long history of protecting consumer privacy on a bi-partisan basis, going back to its efforts to strengthen the 1999 Gramm-Leach-Bliley Financial Modernization Act (GLBA). As passed, GLBA provided for greater privacy protection in the financial marketplace and allowed states to enact stronger financial privacy laws, although the Energy and Commerce committee's laudable additional goal of requiring opt-in consent for data collection and sharing was unfortunately not achieved.[2]

SUMMARY

Consumers today are surrounded by a powerful, sophisticated and ever growing marketing "ecosystem," which collects data from and about them, offline and online, in myriad ways. Collection points include online games, mobile phones, online video, email, display ads, search, in-store transactions, and public records – all these channels are tied together increasingly in real-time updates where users can be bought and sold instantly no matter where they may be. The lesson from the financial meltdown and the new financial law should be that Congress must proactively protect consumers – not as an afterthought. Consumers throughout the country increasingly depend on digital technologies to help them address critical issues related to their finances, health, and families.

---

[1] Web addresses: U.S. PIRG (uspirg.org), Center for Digital Democracy (democraticmedia.org), Consumer Federation of America (consumerfed.org).

[2] Disclosure of Nonpublic Personal Information, Public Law 106-102, 15 U.S.C. § 801-6809, see Section 6807, Relation to State Laws, available at http://www.ftc.gov/privacy/glbact/glbsub1.htm#6807 last visited 21 July 2010) "(b) Greater protection under State law. For purposes of this section, a State statute, regulation, order, or interpretation is not inconsistent with the provisions of this subchapter if the protection such statute, regulation, order, or interpretation affords any person is greater than the protection provided under this subchapter…"

Today, the public has to maneuver through a complex array of increasingly personalized interactive services, including mobile and location-based applications, online videos, and social networks, as they seek information and engage in various transactions. Digital marketing poses new challenges to consumers, since it is able to combine ongoing data collection about individuals as they interact with entertainment or other information. The emergence of mobile and location-based marketing services, which permits the tracking and targeting of an individual in a "hyper-local" geographic area, adds a new dimension to consumer protection issues online. Beyond privacy concerns from data collection, a myriad of complex techniques used to market to consumers—including online "viral" peer-to-peer social media promotions, "smart" ads that learn about an online user so its offer can be changed in real-time, and even the use of neuroscience techniques designed to deliver marketing messages directly into one's subconscious (neuromarketing)—are now regularly in use and can pose real harms.

Financial service advertisers spent some $2.8 billion last year to target U.S. consumers online—for mortgages, credit and credit cards, insurance, and loans for education. A new era in financial marketing has emerged, with consumers increasingly relying on the Internet—including mobile devices—to research and apply for loans, credit, and engage in other financial transactions. While the Internet can help inform consumer decision-making about financial products (and be tremendously convenient), it can also be a confusing—and sometimes intentionally misleading—sales medium. Few consumers are aware of how the online financial marketing system operates, including the role of data collection for targeting an individual consumer for a specific loan or financial product.

To aid in understanding the new system of behavioral targeting in the Internet, last fall our organizations, joined by other leading consumer and privacy organizations, prepared a detailed "Online Behavioral Tracking and Targeting: Legislative Primer." That primer included detailed legislative recommendations, which we incorporate by reference to this testimony.[3]

Consumers need a level playing field at least, in an era where marketers work to 'immerse'' them in applications designed to even subconsciously reveal or provide valuable data. A new law is required, but one which limits overall the data that can be collected from consumers; ensures that consumers have real control when personal data is used for purposes beyond that for which they provided it; and provides for effective enforcement of consumers' rights. The US should work with the EU to develop a meaningful global framework – there is no reason why EU citizens should have greater privacy controls and rights than those in US, and since many of the companies that would be subject to US privacy law also operate on a multinational basis, it would be easier for them to comply with similar standards.

DISCUSSION AND COMPARISON OF THE APPROACHES OF THE TWO ONLINE PRIVACY BILLS BEFORE THE COMMITTEE

In general, while we respect the great deal of thoughtful work that has gone into crafting the two bills before the committee, our initial comment is that they presume the validity of the current system of data collection and are built around that presumption, rather than starting from the place that we would prefer, which is a broader Fair Information Practices-based (FIPs)

[3] The legislative primer is available at http://www.democraticmedia.org/files/privacy-legislative-primer.pdf

framework. To truly protect consumers' privacy, we need to change the paradigm to a more consumer rights-based approach, as we have done with credit reporting, for instance. Commerce will adapt and thrive based on the parameters that public policy sets for consumer privacy.

Put another way, the bills don't track well with a citizen/consumer's rights in such a FIPs framework. The bills don't address the massive growth in data collection, by requiring meaningful data minimization and limits to data retention, for example. The bills largely sanction the existing and worsening regime of ongoing collection, analysis and use of off- and online data, through the industry-preferred regime of notice and choice (not the full FIPs framework). While it is very clear that the Rush Best Practices bill makes a more substantial attempt to comply with more elements of the Fair Information Practices, neither bill is primarily based on a FIPs-framework. Instead, they tend to graft some FIPs rights for consumers and responsibilities for data collectors onto a system that is based on excessive information collection.

We continue to believe that the notice and choice model promotes bureaucracy but does not promote privacy. A privacy bill that actually creates some privacy will need to set strong rules that directly protect consumer privacy, or at least be more firmly based on the Fair Information Practices (FIPs) that have been the foundation of U.S. privacy policy for the past four decades. We believe that the bills should be restructured to follow the FIPs, in much the same way. The bills both make substantial contributions and include many concepts that privacy groups and FTC staff have concluded are key to protecting privacy.

We now will discuss key elements of the bills and make recommendations for improvements.

1) Key Definitions

Covered Information: Both bills include personal identifiers such as the Internet Protocol address in the definition of "covered information." This is crucial, because assumptions can be made about consumers and they can be treated in certain ways based on such identifiers, without the need for other personal information such as a person's name or physical address. The FTC staff report on Behavioral Advertising recognizes the risks posed by IP addresses.[4] Incorporating these findings in legislation enhances consumer protection.

Sensitive Information: The definition of "sensitive information" in the Best Practices Act is better than in Mr. Boucher's discussion draft bill because it is more expansive, especially in the areas of health and finances. For example, "sensitive information" under the Boucher bill includes "medical records, including medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." However, this would not cover situations such as when a consumer researches cancer or another disease online. As that search is not part of "medical records," the information may be collected and used to make judgments about the consumer for any purpose, including employment and insurance. Similarly, the Boucher bill includes information related to financial accounts in the definition of "sensitive information," whereas the Best Practices Act definition encompasses income, assets and liabilities, a broader range of financial information.

[4] FTC Staff Report: Self Regulatory Principles for Online Behavioral Advertising, 21-25, (Feb 2009), http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

We further recommend protection for the sensitive information of adolescents. Adolescents are particularly vulnerable to marketing and profiling.[5] We recommend that sensitive information include age or inferences of age, if under 18, and any information associated with a profile that has age under 18. This will provide protections for those who are marked and targeted as being adolescents.

Operational Purposes: The definition of "operational" in the Best Practices Act is also an improvement over the definition in Mr. Boucher's draft, which is much too vague.

Affiliates and Third Parties: We are pleased that the Best Practices Act takes a slightly different approach to affiliates. Instead of allowing unfettered sharing of covered or sensitive information with affiliates, as Mr. Boucher's draft would do, the Best Practices Act would not allow sharing or use of such information with affiliates if consumers are unlikely to be aware of the affiliation or would not expect that sharing or use to take place. Such affiliates are appropriately treated as Third Parties, which protects consumers better. Business reasons may dictate the presentation of different brand and corporate images to consumers. Legislation which recognizes that businesses create different consumer expectations and loyalties protects consumer expectations and creates incentives for consumers to be properly informed of how their data is shared.

2) The Opt-In and Opt-out Schemes and Exceptions in the Two Bills

We expect industry to push back hard on the very notion of opt-in consent, as (somehow) striking at the very fabric of the economy. We challenge the conventional wisdom that privacy legislation that is based on an opt-in approach is not feasible. There is absolutely no reason why an opt-in approach cannot work, and work well. It is ironic that while many in the business community profess to want to offer consumers real and meaningful control over the collection and use of their data, these same companies and associations are unwilling to provide the most effective means of control for consumers – opt-in. We heard similar objections before the wildly popular national "Do Not Call" registry was implemented, and even after when its legality was unsuccessfully challenged. We were told that it would be the end of direct marketing and that consumers would no longer be able to obtain the products and services they wanted at affordable prices. This was nonsense, as the objection to opt-in is nonsense now. Businesses will become more innovative and responsive to consumers' desires concerning the collection and use of their data if they must first ask for their express affirmative consent. There are those in the industry who have said that privacy legislation ensuring consumers have greater control over their data will actually bolster the online economy. They correctly, in our opinion, see the benefits to brands and advertisers when consumers are more confident about how their information is being treated online.[6]

We are pleased that in both bills, consumers' affirmative consent – opt-in – is required if a change in a covered entity's privacy policy means that covered or sensitive information previously collected about consumers could be used or shared in a manner not previously disclosed.

---

[5] *See* Comments of CDD, et. al., COPPA Rule Review, 40-43 (June 2010), http://www.ftc.gov/os/comments/copparulerev2010/547597-00046-54855.pdf.
[6] See http://www.digidaydaily.com/stories/the-boucher-bill-right-on-time/.

Congress should recognize that in today's data collection environment, consumers face practically insurmountable obstacles when it comes to comprehending—let alone controlling—how and why their information (including on their behaviors) is being collected, analyzed and used. Research from leading privacy academics has demonstrated that the current reliance on privacy policies, which in effect buries clear disclosure in a form of digital fine print, doesn't help inform consumers. Even if the FTC, as proposed by the bill introduced by Chairman Rush, develops a new standard for such notices, many privacy and consumer experts believe that they will do little to actually help consumers maneuver through a system purposely designed to encourage them to consent to data collection. That is why most of the leading consumer and privacy groups support an opt-in regime for the collection of information. An opt-out regime will not stem the data collection tide that threatens consumer interests

If secondary use of consumers' personal information can truly benefit them, why shouldn't covered entities be required to explain exactly how and obtain their affirmative consent? We recommend that non-sensitive information should only be allowed to be collected and used for non-operational purposes for 24 hours, after which opt-in consent would be required to continue to store and use it.

We also recommend that Congress consider mandating the creation of a "Do Not Track" registry to provide consumers with an easy-to-use, effective means of controlling the most invisible collection and use of their personal information, behavioral tracking and targeting. This is when information about their online and offline activities is used to build profiles of them for marketing and other purposes. The assumptions made about consumers through behavioral tracking may be inaccurate – who among us has not searched online for information about a friend or relative's health problems, or purchased something for another person that we would not have bought for ourselves? And some consumers may simply not want to be tracked on principle. Consumers should be able to avoid all behavioral tracking and targeting if they wish through one easy step. This would work in much the same way as the federal "Do Not Call" registry, except that instead of consumers putting their own Internet Protocol Addresses in the registry, entities that engage in behavioral tracking and targeting would submit the technical information to the registry that would enable consumers to block those activities. The FTC can consult with experts to build such a system.

But even with the required notice and opt-in, consumers may not be able to fully appreciate how information about their health, finances, race or ethnicity, sexual orientation, religious beliefs, political beliefs and data about their location might be accessed and used, for purposes they never anticipated. For instance, a consumer searching for mortgage information is unaware that she is being tracked as she searches for the best deal online and that her "profile" may contain information about her race, ethnicity, financial condition, health concerns, where she travels, and other sensitive information that can influence the kinds of offers and products that she may receive. We commend the bills for advancing safeguards related to sensitive information, although more protections are required. Many consumer and privacy groups are especially pleased that the bills declare racial/ethnic and sexual orientation related information as sensitive data. We applaud that strong safeguard as a significant advance to protect consumers and citizens from emerging new forms of racial and other types of profiling that we believe can be used to discriminate against them, including involving issues of critical importance to their welfare. We know that in particular, Chairman Rush has been publicly concerned about these issues, and we

wish to take this opportunity to also thank him for his leadership on this issue. We commend both bills for inclusion of geolocation information—a critical consumer protection advance that recognizes that in this new era of "smart" phones and what's called hyper-local targeted marketing, it is essential that such highly private information is completely under the control of the individual. As we explained in a complaint[7] filed last year at the FTC, today's mobile marketing environment combines information about one's behavior [behavioral targeting] with knowledge of a consumer's actual location. Geolocation information, including the history of where we and our families spend time, requires the highest form of consumer privacy control.

But we also strongly urge the Committee to strengthen its protections for sensitive information. As we have explained to the FTC and other federal agencies, consumers are unaware about the data collection and behavioral marketing processes that now underlie their activities involving such sensitive transactions as using the Internet to research and then pursue financial transactions, including mortgages and other forms of loans and credit. Nor are they likely to recognize that when investigating concerns about a medical issue, they can become the subject of what's called "condition targeting" by the online health marketing industry. Chairman Rush's bill correctly requires the FTC to conduct a specific rule-making on the issue of sensitive data, to potentially amplify what subjects and areas should also be included. While we greatly support this provision, we hope we can work with this committee, Chairman Boucher, and other members to strengthen the section on what should be included in this extremely critical to consumer welfare section.

We also note that storing and sharing sensitive information puts consumers at risk of identity theft and other crimes. To truly protect consumers, legislation should prohibit sensitive data from being collected or used for any purposes other than for the transactions for which they have been provided. The bill just introduced by Chairman Rush requires third parties to only use sensitive data based on affirmative opt-in consent for a specific purpose only—which we support. The use of sensitive data by first parties should be granted narrowly as well, for a limited specific purpose.

We recommend that non-sensitive information should only be allowed to be collected and used for advertising purposes for 24 hours, after which opt-in consent would be required to continue to store and use it. We believe that consumers should be given as complete control over the data collection, profiling and targeting process. Not everyone will wish to participate in so-called "Safe Harbor" approaches and other longer forms of opt-out. Data collection, profiling and targeting practices beyond an initial 24 hour period for non-sensitive information should require affirmative consent from a consumer.

[7] Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices, Center for Digital Democracy and U.S. PIRG January 2009, (available at http://www.democraticmedia.org/files/FTCmobile_complaint0109.pdf)

3) Access, Correction, Data Retention and Other FIPs Issues

We note that neither bill requires covered entities to limit the collection of personal information to that which is necessary for the transaction or activity in which the consumer is engaging – a fundamental element of the Fair Information Practices. This, again, is why opt-in should be the standard, not-opt-out, when information will be used for secondary purposes. There is also no limit to the amount of time that covered or sensitive information can be retained and used, beyond an 18-month retention limit for managed profiles in Mr. Boucher's bill. The Federal Trade Commission should be instructed to set reasonable retention limits.

We are pleased that the Rush Best Practices Act addresses the issue of access and correction for consumers, another important Fair Information. Legislation must ensure a consumer's right to not only access their profile and related information, but a fair process where they have the right to delete incorrect data, yet neither bill provides this protection.

We are also pleased to see the provisions in the Best Practices Act for data security and privacy risk assessments.

4) Concerns about Use of Aggregated and Re-Identified Information:

We are pleased that provisions in the bill by Chairman Rush to establish safeguards for the use of so-called re-identified data, designed to prevent the reconstructing of information on a consumer. However, in today's advanced data mining and informational targeting environment, so-called aggregate information can help provide a detailed analysis of a consumer. The FTC should be authorized to conduct a rulemaking on the appropriate use of aggregate and so-called de-identified data that would both articulate best industry practices and establish the necessary consumer privacy safeguards.

5) Use of Consumer Profiles and Discussion of Issues of Consumer Harms

Members of the data collection industry, including digital marketers, have established a far-reaching system of consumer profiling. Today, as we have discussed, so-called real-time ad auctions actually sell access to our online profiles to the highest bidder. Consumers require a system where such profiles are closely analyzed and assessed, including by regulators. The propriety of the online profiling system for consumer targeting—now across the offline and online platforms, including mobile—must be questioned. We urge the committee to require the FTC to engage in a Rulemaking on the issue of profiles and what are appropriate policies for their role. We especially suggest the FTC be mandated to examine how the use of online profiles raises consumer protection concerns in such areas as health and financial transactions a consumer makes.

6) Concerns About "Publicly Available Information"

We are concerned that this provision creates an unfortunate loophole which sanctions the collection and use of greater amounts of data on an individual consumer. As the Chairman and the committee recognize, in today's online environment information about us is often made available without the consumer realizing that it will be swept into a profile or some other form of commercial database. If we pose a picture of our friends at some celebration on our social

network, and we are toasting the birthday of a friend, should that be included in what's to be considered a database for commercial use? There should be meaningful limitations on what is considered publicly available information in this new era. The FTC should be empowered to conduct a rulemaking to set reasonable limits that will protect consumers.

7) Concerns About the Self-Regulatory Safe Harbor Scheme

We are concerned about the Rush safe harbor provision for covered entities that participate in self-regulatory programs because experience has shown that such programs have fallen far short of ensuring adequate protection for the privacy and security of consumers' personal information in the past. While that safe harbor provision – including its universal opt-out requirement -- in the Best Practices Act is more robust than the exception in Mr. Boucher's discussion draft for entities that participate in self-regulatory programs, it needs to be significantly strengthened if it is retained in the legislation. As do too many other parts of the bill, the system relies extremely heavily on FTC rulemaking and enforcement, rather than on more specific guidelines and private rights of action. Any measure that provides for FTC-approved self-regulatory programs must require the FTC to closely monitor and test those programs, rather than relying on the program operators to test and monitor themselves.

We note that evidence from the Federal Trade Commission's previous encouragement of self-regulatory schemes is not promising. As Hoofnagle,[8] (2005), notes:

> "In 2000, a 3-2 majority of the FTC formally recommended that Congress adopt legislation requiring commercial web sites and network advertising companies to comply with Fair Information Practices. However, a year later with the appointment of a new FTC Chairman, the FTC embraced self-regulation again."

He then goes on to say:

> "The overall effect of the FTC's [self-regulatory] approach has been to delay the adoption of substantive legal protection for privacy. The adherence to self-regulatory approaches, such as the Network Advertising Initiative that legitimized third-party Internet tracking and the Individual References Service Group principles that concerned sale of SSNs, allowed businesses to continue using personal information while not providing any meaningful privacy protection. Ten years later, online collection of information is more pervasive, more invasive, and just as unaccountable as ever—and increasingly, the public is anesthetized to it."

Similarly, Dixon[9] (2007) found the following, in a report on the Network Advertising Initiative (NAI):

---

[8] Hoofnagle, Chris Jay, Privacy Self Regulation: A Decade of Disappointment (January 19, 2005). Available at SSRN: http://ssrn.com/abstract=650804 or doi:10.2139/ssrn.650804

[9] Dixon, Pam, Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation, World Privacy Forum, (November 2007). Available at http://www.worldprivacyforum.org/pdf/WPF_NAI_report_Nov2_2007fs.pdf

> The NAI has made no attempt to extend its self-regulatory structure to reflect developments in the Internet sector or in business practices. Its conception of online profiling grew rapidly stale. For example, techniques exist today for tracking of consumers that do not rely on traditional cookies. As time passed, the NAI self-regulation's effectiveness toward consumer protection became less effective or and less relevant.

We are encouraged by the efforts of the current FTC to study behavioral targeting, hold workshops and make positive recommendations.[10] Nevertheless, the FTC's historic efforts at replacing privacy protection with privacy self-regulation have not been positive. Robust rules based on Fair Information Practices are required.

8) The Bills Need Stronger Private Rights of Action

The Boucher bill (section 9) would block consumers from taking legal action to enforce their rights. As you know, federal and state agencies play important roles in protecting the public, but they cannot and do not take action to resolve every situation in which consumers' rights have been violated. It is essential for individuals to be able to enforce their privacy rights and stop egregious practices. A private right of action must be provided to help ensure a level playing field and incentivize companies to respect and protect consumers' privacy.

While the Rush bill grants very limited private rights of action for certain **willful** violations (a high standard), why not give consumers full legal rights to enforce the law?

Instead, both these bills bow to industry demands to limit consumer rights to police the marketplace. Private rights of action are not designed – as industry rhetoric would have you believe – to enrich trial lawyers. Rather, the threat of a private right of action deters unsavory practices and encourages compliance with the law. Conversely, the lack of private rights of action encourages companies to ignore the law.

The marketplace functions best when consumers, federal agencies and state attorneys general can all enforce strong laws, and states can enact stronger laws when new or local threats emerge.

9) The Bills Need Stronger State Enforcement and Less Preemption

We are very concerned about the sweeping preemption in the current draft of the Boucher/Stearns legislation. The bill preempts state or local laws or regulations that include "requirements for the collection, use, or disclosure of covered information." This is incredibly broad and could block existing or new measures on the state level to limit the use of certain types of information, such as Social Security numbers, to notify consumers of data breaches, to protect health data, and to extend other needed privacy protections to consumers.

While the Rush draft incorporates a narrower form of preemption, its provisions are still problematic. Rather than a broad preemption, we recommend that any final bill set minimum

---

[10] See, eg, Remarks of David Vladeck, Director, Bureau of Consumer Protection, Exploring Privacy: A Roundtable Series, Berkeley, CA (28 January 2010) available at http://www.ftc.gov/speeches/vladeck/100128exploringprivacy.pdf

standards for privacy protection and allow states to create stronger laws and regulations to safeguard consumer data against misuse and abuse if necessary. The stronger the final bill is, the less likely that there will be any significant gaps that states will feel compelled to fill.

We also believe that state attorneys general should always have the ability to enforce the federal law, or their state laws, and then in either state or federal court, and not be restricted to federal courts.

10) **Other Concerns (Lack of A Findings Section)**

We believe that there should be a strong findings section at the beginning of the bills. We urge you to carefully review our suggestions, as we are working toward the same goal: to protect the interests of Americans while maintaining and increasing robust commerce. In fact, providing meaningful protection for consumers' data is necessary in order to ensure their confidence in our increasingly complex marketplace. The argument that we must choose between privacy or access to a broad array of reasonably attainable goods and services is false. American business can deliver both, and we should demand no less.

CONCLUSION

We commend Chairmen Rush and Boucher, along with Ranking Member Stearns (and other members of the committee), for helping advance a much needed legislative debate about the best way to protect consumer privacy. Consumer and privacy groups recognize the important role that online marketing and advertising play, as a source of revenues for online and other publishing, and as a robust sector of the digital economy. We also recognize that data collection, online and offline, plays an important role—perhaps the most critical one---for the industry's future.

But contemporary data collection practices, especially online, far surpass what consumers may have become familiar with on a day-to-day basis. Not only are our behaviors online closely tracked and analyzed (such as the content we like or tend to avoid; what we are willing to pay for or what we discard from online shopping carts), but consumers are confronted with an array of interactive ads purposely designed to elicit, sometimes subconsciously, greater amounts of our data. Today, as U.S. PIRG, Center for Digital Democracy and others recently filed at the FTC, so-called real-time ad exchanges auction consumers off to the highest bidder, so that they can be targeted for marketing wherever they might happen to be online. All this is done in a non-transparent, unaccountable manner, without the consumers' knowledge or consent.

A vast, automated, and powerful data collection complex has emerged, capable of generating and continually revising a profile—a consumer X-Ray—of our habits, interests, worries, financial status, families. These applications can hone in on an individual consumer, and almost instantly create an interactive ad that continues to transform itself as it stealthily "learns" about the interests of a single consumer. Google's recent acquisition of Teracent, one of the companies focused on so-called "Smart" ads, is just one example of why online marketing's ability to encourage a consumer to provide data demands a rigorous framework to protect consumer privacy. As the company explains, "Teracent deploys an unlimited number of ad creative combinations (using your catalogs, databases, images, and messages) through a single ad unit. Then, sophisticated machine learning algorithms instantly select the optimal creative elements

for each ad impression – based upon a real-time analysis of which items will convert from impressions into sales."[11]

We firmly believe that the U.S. should be the global leader in creating a policy framework shaped by FIPs that greatly aids the growth of the digital marketing industry. While advances in so-called computational advertising reflect an important contribution to innovation and can help spur the growth of ad revenues, they must be guided by a framework grounded in the requirements of consumer protection in a democratic society. That's why we—consumer and privacy groups and other concerned citizens—want to work with Chairman Rush, Chairman Boucher, Ranking Members Stearns and Radanovich—as well as Chairman Waxman and Ranking Member Joe Barton, Mr. Markey and others—to build up these initial proposals, and to work with industry, academic experts, and other stakeholders to develop legislation that is grounded in Fair Information Practices.

Among the key elements of a revised bill is a framework focused on overall data minimization. Today, anyone who knows the online and offline data collection industry will tell you the focus is on data maximization. "Every move you make," as the lyrics of the Police song go, could be the data collection industry theme song, as we are all being watched, compiled, analyzed and then acted upon. While tools involving opt-in and safe harbors, for example, provide greater control by a consumer, they do not constrain the dramatic and far-reaching growth of online and offline data collection for personalized and interactive targeting. Although the bill offered by Chairman Rush incorporates a key section on data minimization, we believe that the overall legislation should focus on mandating that less data be collected wherever possible. The online and data collection industry should not be permitted to engage, as they are, in an unchecked data "arms race." Digital data détente is required, with a system based on minimal data collection, complete transparency, consumer control and redress, and federal, state and private rights of enforcement.

OTHER BACKGROUND SECTIONS

Attachments:
Appendix 1: The Need For Privacy Protection To Be Based On The Fair Information Practices (Page 12)
Appendix 2: Interactive Advertising Data Collection Examples (3 pages, Pages 13-15)
Appendix 3: A Marketer's Guide to Understanding the Economics of Digital...2009, AAAA. (Page 16).

[11] Teracent, "Advertiser Solutions," http://www.teracent.com/advertiser-solutions/ (viewed 20 July 2010).

Appendix 1: The Need For Privacy Protection To Be Based On The Fair Information Practices

In 1973, a task force was formed at the U.S. Dept. of Health, Education and Welfare (HEW) to look at the impact of computerization on medical records privacy. The members wanted to develop policies that would allow the benefits of computerization to go forward, but at the same time provide safeguards for personal privacy.

The task force developed a Code of Fair Information Practices, consisting of five clauses: openness, disclosure, secondary use, correction, and security. At the same time, Sweden enacted a law that codified many of the same fair information principles formulated by the HEW.

In the ensuing years, other European countries enacted similar omnibus data protection laws. And in 1980, the Organization of Economic Cooperation and Development (OECD), an international body based in Paris, adopted the "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data."

In general, consumer and privacy organizations consider the OECD Guidelines to be the most robust version of the Fair Information Practices. Many industry self-regulatory organizations have adopted notice and choice regimes that, at best, amount to “FIPs-Lite” and at worst to bureaucracy without privacy protection. For the record, the OECD Guidelines are listed below.

Privacy Guidelines
Organization of Economic Cooperation and Development, 1980

From "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," OECD, 1980.[12]

Collection Limitation. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
Data quality principle. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.
Purpose specification. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
Use limitation principle. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [Purpose specification] except:
(a) with the consent of the data subject; or
(b) by the authority of law.
Security safeguards principle. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
Openness principle. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity about usual residence of the data controller.
Individual participation principle. An individual should have the right:
(a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
(b) to have communicated to him, data relating to him
1. within a reasonable time; 2. at a charge, if any, that is not excessive; 3. in a reasonable manner; and 4. in a form that is readily intelligible to him;
(c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
(d) to challenge data relating to him and, if the challenge is successful, to have the data erased; rectified, completed or amended.
Accountability principle. A data controller should be accountable for complying with measures which give effect to the principles stated above.

[12] Available at http://bit.ly/coc5sq (last visited 10 July 2010).

Appendix 2: Interactive Advertising Data Collection Examples[13]

1. Consumer tracking online:
As Yahoo's online ad auction service Right Media explains in a "primer" for data providers: "Data providers are changing the advertising landscape by focusing on who sees ads rather than where ads appear. Here is how it works: When consumers go to certain web sites, the page places a tag (or 'cookie') within the browser—tracking that a particular browser visited a particular site. In some cases, a data provider (which can also be described as a data 'collector') pays the web site for the ability to do this. The cookie enables the data provider to follow consumers and track their online 'behavior.'"

2. *New York Times* description of real-time ad-bidding process:
"Now, companies like Google, Yahoo and Microsoft let advertisers buy ads in the milliseconds between the time someone enters a site's Web address and the moment the page appears. The technology, called real-time bidding, allows advertisers to examine site visitors one by one and bid to serve them ads almost instantly…. Using data providers like BlueKai or eXelate, AppNexus can add information about what a person has been doing online. 'It's a lot about being able to get the right users, but it's also about passing on certain instances where we don't think you're in the market, based on what you've been doing in the past hour,' Mr. Ackley [vice president for Internet marketing and advertising at eBay] said…. Until the arrival of real-time bidding, said Mr. Mohan of Google, 'the technology hasn't really been there to deliver on the promise of precise optimization, delivering the right message to the right audience at the right time' in the display world."

3. Online tracking now combined with offline databases to create detailed profiles:
"Digital-marketing companies are rapidly moving to blend information about consumers' Web-surfing behavior with reams of other personal data available offline, seeking to make it easier for online advertisers to reach their target audiences…. eXelate will tie its data on more than 150 million Internet users to Nielsen's database, which includes information on 115 million American households, to provide more-detailed profiles of consumers. 'We can build [consumer] profiles from any building blocks,' says Meir Zohar, chief executive of eXelate…. 'Age, gender, purchase intent, interests, parents, bargain shoppers—you can assemble anything.'" eXelate "gathers online consumer data through deals with hundreds of Web sites. The firm determines a consumer's age, sex, ethnicity, marital status and profession by scouring Web-site registration data. It pinpoints, for example, which consumers are in the market to buy a car or are fitness buffs, based on their Internet searches and the sites they frequent. It gathers and stores the information using tracking cookies, or small strings of data that are placed on the hard drive of a consumer's computer when that consumer visits a participating site. Advertisers, in turn,

---

[13] These examples are derived from Center for Digital Democracy, U.S. PIRG et al complaints to the Federal Trade Commission on Online Marketing. See April 2010, Complaint - Real-time Targeting & Auctioning, Data Profiling, Optimization, And Economic Loss To Consumers & Privacy (available at http://www.democraticmedia.org/files/u1/20100407-FTCfiling.pdf) and also January 2009, Complaint and Request for Inquiry and Injunctive Relief Concerning Unfair and Deceptive Mobile Marketing Practices (available at http://www.democraticmedia.org/files/FTCmobile_complaint0109.pdf) for our most recent filings.

purchase cookie data from eXelate and use it to buy targeted online ads." eXelate's recent agreement with Nielsen will "will allow advertisers to go to eXelate to buy New York-based Nielsen's trove of data converted to a cookie-based digital format. That data comes from sources including the Census Bureau, the firm's own research and that of other consumer-research firms, such as Mediamark Research and Experian Simmons."

4. Ad exchange targeting involves such sensitive areas as health and finance:
Google's DoubleClick Ad Exchange permits the targeting of a wide range of health and financial behaviors. These include arthritis, diabetes, GERD and digestive disorders, migraines, sleep disorders, pain management, credit cards, loans and insurance.

5. Social Media marketing includes online discussions of personal health:
Social media marketing is a recent form of interactive advertising that takes advantage of a person's social relationships online—their so-called social graph—with brands and other advertising. Through various techniques and technologies, companies monitor consumer conversations about a product or medical condition, often covertly. Heartbeat Digital's BuzzScape, for example, "allows clients to monitor discussions that flow in and out of the tens of thousands of message boards, forums, blogs and social networks that increasingly dominate the online environment. 'We translate 'buzz' into ROI,' said Bill Drummy, chairman and CEO of Heartbeat. 'In a sense, we eavesdrop on public conversations among people with a shared interest, then use what we learn to create interactive marketing campaigns that address the identified needs, wants and gaps in knowledge of target audiences.'"

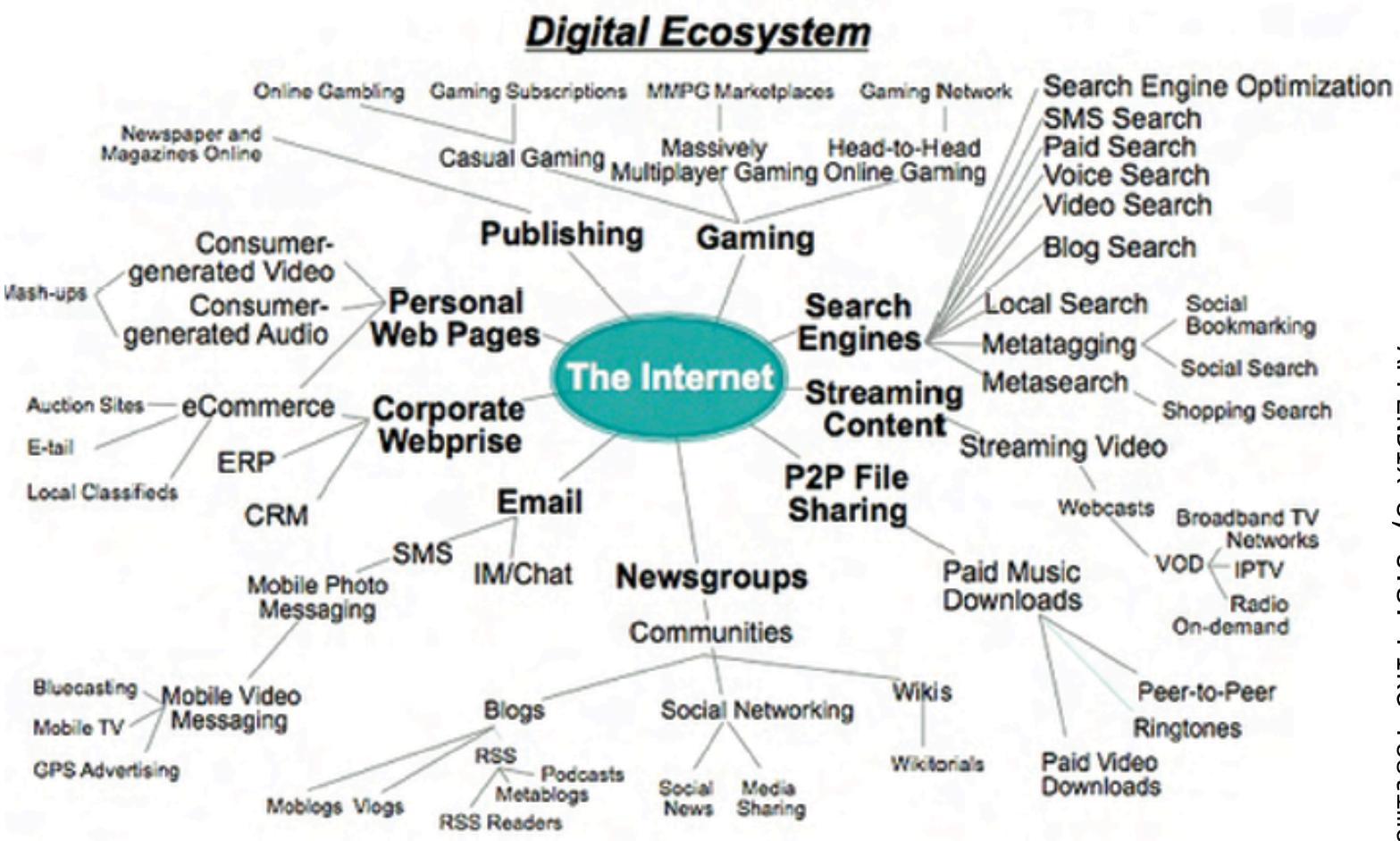
6. Even on so-called "opt-in" sites that require registration, consumers may not be fully aware of the amount and range of personal information that they are sharing with third parties:
PatientsLikeMe offers a new service, PatientsLikeMeListen, to its industry partners. In addition to giving pharmaceutical companies "unprecedented insight on how your brand is perceived," the monitoring service also provides startling amounts of personal data about the online conversants, including gender, age, time on treatment, time since diagnosis, disease progression, disease type, symptomology, longitudinal variation, and supporting therapies. As Razorfish's Debrianna Obara explains, "Sites such as Yahoo!, EverydayHealth and MSN are able to segment their audience differently. Since most of their users have created accurate profiles of themselves when they register with a site (including birth year, number of children in household, zip code, and ailments in the household), these sites can create packages for advertisers comprised only of people that fit the desired audience profile.

7. Mobile marketing poses new threats to consumer privacy:
Mobile devices, which know our location and other intimate details of our lives, are being turned into portable behavioral tracking and targeting tools that consumers unwittingly take with them wherever they go. Bango's Sarah Keefe notes how online marketers will be able to update profile-based mobile targeting in real time: "Marketers can…compile an accurate and rich understanding of their target consumer's profile. With this data jackpot, marketers can target messages to the right audience in the right geographic location. Also, real time data allows campaigns to be tweaked and refined to ensure success and optimize the marketing investment…. It's a brave new mobile marketing world out there and the wealth of data and analytics capabilities that are part of the new landscape eliminate the risk of jumping right in. Why wait?" As Mobixel reveals in its product literature, "the opportunity to reach a large

captive audience" through mobile advertising is "extremely enticing," because "the mobile phone offers focused demographic, behavioral and contextual targeting and immediate engagement." Using these capabilities, its Mobixel Ad-It service provides the tools for mobile network operators to "gather, quantify and analyze" a wide range of information about subscribers, including "demographic details, service profiles, behavioral patterns, as well as the real-time context of services, location and device and network capabilities…. It then uses this information, in real time, to make complex targeting decisions" on behalf of advertisers.

8. Location-based targeting adds a new threat to consumer privacy:
If behavioral targeting is a potent force in interactive advertising, the mobile marketplace increases the power of such targeting still further by pinpointing the precise location where various consumer behaviors take place. In the past, of course, marketers could determine the approximate location of mobile device users through a complex system of triangulation. But the latest generation of cellular phones, which are increasingly equipped with sophisticated global positioning capabilities, are taking all of the guesswork out of location-based targeting. Utilizing these advances in GPS technology, marketers can now determine the precise location of mobile users—within three feet. As Ad Age noted, "Context-based banner ads now morph into GPS locators for the closest product from the user's current location. Ads can initiate calls or purchase DVDs for instant viewing. Ads can incorporate audio, video and web browsing, and can also direct users to the iPhone App Store or iTunes."

9. Online "lead generation" in financial services:
The role of online lead generation (so-called "trigger leads") and the use of behavioral targeting for mortgages and other loans represent a potentially critical threat to the privacy of digital consumers, whose data are used without their clear understanding, let alone control, of such surveillance. For example, Lightspeed Research promises marketers a "full wallet view across customers' many financial services relationships," providing "unparalleled insight into consumers' use of credit, debit, banking and alternative payment products. We passively gather information from their financial accounts and merge it with third-party behavioral datasets, survey-based attitudinal insights, and industry expertise."



Source: *A Marketer's Guide to Understanding the Economics of Digital*…..2009, AAAA.